UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/632,135	07/30/2003	Siani Lynne Pearson	B-5196 621146-3	1838

7590 06/20/2008

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	PAPER NUMBER
2132	
MAIL DATE	DELIVERY MODE
06/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/632,135	PEARSON ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 June 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12,14-33 and 35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12, 14-33 and 35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment after a non-final rejection filed on June 29, 2007. Claims 13 and 34 are canceled. Thus claims 1-12, 14-33 and 35 are pending/examined. Every independent claim 1, 14, 15, 17, 23 and 35 is amended.

2. The amendment made to the respective independent claims overcomes the 101 rejection set forth in the previous office action. Thus the previous 101 rejection set forth in the previous office action is withdrawn.

Response to Arguments

3. Applicant's arguments filed on June 29, 2007 have been fully considered but are moot in view of the new ground(s) of rejection.

Priority

4. Receipt is acknowledged of papers submitted under 35 U.S.C. 119 (a)-(d), which papers have been placed of record in the file

Claim Rejections - 35 USC § 102

6. Claim 15 is rejected under 35 U.S.C. 102(e) as being anticipated by England et al. (hereinafter referred as England) (U.S. Patent No: 6, 327,652 B1) (Filed on Jan 8, 1999), which Claims Priority from Provisional Application No 60,105,891 filed on October 26, 1998)

7. **<u>As per independent claim 15</u> England discloses a method of validating the performance of an entity in a first computing environment** [Column 9, lines 65-column 10, lines 3] *(The content provider 220 examines the CPU certificate 202, the DRMOS identity 206, and the properties specified in the rights manager certificate 210 to determine whether it should establish a trust relationship with the DRMOS 205 on the subscriber computer 200/entity in a first computing environment).*, **comprising**

issuing a first challenge to determine if a computing environment of the entity is trustworthy and to determine the integrity of an application run in the entity's computing environment if the entity is determined to be trustworthy, [Column 9, line 45-lines 51 and column 9, lines 65-column 10, lines 3; column 9, lines 27-29**]** ***(****The content provider 220 transmits a challenge message 4 to the DRMOS 205 asking for the identity of the CPU 201, the DRMOS 205, and the application 209. The DRMOS 205 transmits a response message 5 containing a certificate 202 for the CPU 201, its own identity 206, and the rights manager certificate 210 for the application 209.Furthermore on column 9, lines 65-column 10, lines 3, the following has been disclosed. "The certificate 202 is signed using the private key of the CPU 201. The content provider 220 examines the CPU certificate 202, the DRMOS identity 206, and the properties specified in the rights manager certificate 210 to determine whether it should establish a trust relationship with the DRMOS 205 on the subscriber computer 200." Note that as it is described*

on column 9, lines 27-29, certificate 210 identifies the trusted application)

and

allowing the entity access to the first computing environment based on a response to the challenge received from the entity. [Column 9, lines 65-column 10, lines 3] *(The certificate 202 is signed using the private key of the CPU 201. The content provider 220 examines the CPU certificate 202, the DRMOS identity 206, and the properties specified in the rights manager certificate 210 to determine whether it should establish a trust relationship with the DRMOS 205 on the subscriber computer 200.)*

Claim Rejections - 35 USC § 103

9. **Claims 1-12, 14, 16-33 and 35** are rejected under 35 U.S.C. 103(a) as being unpatentable over the publication with the title "Building A Foundation of Trust in the PC" (The Trusted Computing Platform Alliance) (hereinafter refereed as **Trusted Computing**) (Printed publication date: January, 2000) (Submitted with IDS) in view of England et al. (hereinafter referred as England) (U.S. Patent No: 6, 327,652 B1) (Filed on Jan 8, 1999), which Claims Priority from Provisional Application No 60,105,891 filed on October 26, 1998)

10. **As per independent claims 1, 14, 17, 23 and 35 Trusted Computing discloses a method of validating the performance of a participant in an interactive computing environment,** *[See page 5, under the title "Remote Attestation up to page 6, first paragraph]* **comprising**:

Issuing a first challenge to a participant's computing device; receiving a first response from the participant's computing device in response to the first challenge; determining whether the participant's computing device is trustworthy, based on the first response; *[See page 5, under the title "Remote Attestation, up to page 6, first paragraph] ("TCPA remote attestation allows an application* ***(the "challenger")*** *to trust a remote platform. This trust is built by obtaining integrity metrics for the remote platform, securely storing these metrics and then ensuring that the reporting of the metrics is secure. For example, before making content available to a subscriber, it is likely that a service provider will need to know that the remote platform* ***is trustworthy.*** *The service provider's platform (the "challenger") queries " the remote platform, meets the limitation "****issuing a first challenge to a participant's computing device to determine whether the participant's computing device is trustworthy****," During system boot, the challenged platform creates a cryptographic hash of the system BIOS, using an algorithm to create a statistically unique identifier for the platform. The integrity metrics are then stored. When it receives the query from the challenger, the remote platform responds by digitally signing and then sending the integrity metrics. The digital signature prevents tampering and allows the challenger to verify the signature. If the signature is verified, the challenger can then determine whether the identity metrics are trustworthy meets the limitation of* ***"determining whether or not the participant's computing device is trustworthy"*** *If so, the challenger, in this case the service provider, can then*

deliver the content. It is important to note that the TCPA process does not make judgments regarding the integrity metrics. It merely reports the metrics and lets the challenger ***make the final decision regarding the trustworthiness*** *of the remote platform.)*

Trusted Computing is silent on,

- issuing a second challenge to the participant's computing device if the participant's computing device is determined to be trustworthy; receiving a second response from the participant's computing device in response to the second challenge; testing the integrity of an application running on the participant's computing device based on the received second response; allowing the participant's computing device access to a computing environment based on the test results .

- **However, in the same field of endeavor England, on** Column 9, line 45-lines 51 and column 9, lines 65-column 10, lines 3; column 9, lines 27-29 **discloses the following which meets the above limitation. First on column 9, lines 45-lines 51 the following has been disclosed.** *The content provider 220 transmits a challenge message 4 to the DRMOS 205 asking for the identity of the CPU 201, the DRMOS 205, and the application 209* and this meets the limitation recited as "issuing a second challenge to the participant's computing device if the participant's computing device is determined to be trustworthy" because all subscribers shown on figure 2, ref. Num "200" provides some information to content providers shown on figure 2, ref. Num 220, before they receive any challenge from the content providers that will qualify them to be trustworthy; Furthermore *The DRMOS 205 transmits a*

response message 5 containing a certificate 202 for the CPU 201, its own identity 206, and the rights manager certificate 210 for the application 209.Furthermore on column 9, lines 65-column 10, lines 3, the following has been disclosed. "The certificate 202 is signed using the private key of the CPU 201. The content provider 220 examines the CPU certificate 202, the DRMOS identity 206, and the properties specified in the rights manager certificate 210 to determine whether it should establish a trust relationship with the DRMOS 205 on the subscriber computer 200." Note that as it is described on column 9, lines 27-29, certificate 210 identifies the trusted application)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to employ the teachings o**f England** such as issuing a second challenge to the participant's computing device if the participant's computing device is determined to be trustworthy; receiving a second response from the participant's computing device in response to the second challenge; testing the integrity of an application running on the participant's computing device based on the received second response; allowing the participant's computing device access to a computing environment based on the test results **within the method of Trusted Computing** for the purpose of creating more secure, comprehensive, software identification method that enforces digital rights. [See "England", column 1, lines 21-23]

11. **<u>As per claims 2-4, 18-20 and 24-26, the combination of</u> Trusted Computing and England discloses a method as applied to claims above. Furthermore England discloses a method, in which the**

second challenge tests for modification of the application. [Column 9, line 45-lines 51 and column 9, lines 65-column 10, lines 3; column 9, lines 27-29**]** ***(England, on*** *Column 9, line 45-lines 51 and column 9, lines 65-column 10, lines 3; column 9, lines 27-29* ***discloses the following which meets the above limitation. First on column 9, lines 45-lines 51 the following has been disclosed.*** *The content provider 220 transmits a challenge message 4 to the DRMOS 205 asking for the identity of the CPU 201, the DRMOS 205, and the application 209 and this meets the limitation recited as "issuing a second challenge to the participant's computing device if the participant's computing device is determined to be trustworthy" because all subscribers shown on figure 2, ref. Num "200" provides some information to content providers shown on figure 2, ref. Num 220, before they receive any challenge from the content providers that will qualify them to be trustworthy"; Furthermore The DRMOS 205 transmits a response message 5 containing a certificate 202 for the CPU 201, its own identity 206, and the rights manager certificate 210 for the application 209.Furthermore on column 9, lines 65-column 10, lines 3, the following has been disclosed. "The certificate 202 is signed using the private key of the CPU 201. The content provider 220 examines the CPU certificate 202, the DRMOS identity 206, and the properties specified in the rights manager certificate 210 to determine whether it should establish a trust relationship with the DRMOS 205 on the subscriber computer 200." Note that as it is described on column 9, lines 27-29, certificate 210 identifies the trusted application)*

12. **<u>As per claims 5-10, 21-22 and 27-28 the combination of</u> Trusted Computing and England discloses a method as applied to claims above. Furthermore Trusted Computing discloses a method, in which in the first challenge the trustworthiness of the BIOS is validated,** *[See page 5, under the title "Remote Attestation, up to page 6, first paragraph] ("TCPA remote attestation allows an application* ***(the "challenger")*** *to trust a remote platform. This trust is built by obtaining integrity metrics for the remote platform, securely storing these metrics and then ensuring that the reporting of the metrics is secure. For example, before making content available to a subscriber, it is likely that a service provider will need to know that the remote platform* ***is trustworthy.*** *The service provider's platform (the "challenger") queries " the remote platform, meets the limitation "****issuing a first challenge to a participant's computing device to determine whether the participant's computing device is trustworthy****," During system boot, the challenged platform creates a cryptographic hash of the system BIOS, using an algorithm to create a statistically unique identifier for the platform. The integrity metrics are then stored. When it receives the query from the challenger, the remote platform responds by digitally signing and then sending the integrity metrics. The digital signature prevents tampering and allows the challenger to verify the signature. If the signature is verified, the challenger can then determine whether the identity metrics are trustworthy meets the limitation of* ***"determining whether or not the participant's computing device is trustworthy"*** *If so, the challenger, in this case the service provider, can then*

deliver the content. It is important to note that the TCPA process does not make judgments regarding the integrity metrics. It merely reports the metrics and lets the challenger ***make the final decision regarding the trustworthiness*** *of the remote platform.)*

13. **<u>As per claims 11-12,16, 29-33</u> the combination of Trusted Computing and England discloses a method as applied to claims above. Furthermore England discloses a method, in which the challenge is issued by a server** *[figure 2, ref. Num "220" or "Content Provider"]* **with which the participants computing device** *[figure 2, ref. Num "200"/Subscribers]* **is in communication.[Figure2] (**Column 9, line 45-lines 51 and column 9, lines 65-column 10, lines 3; column 9, lines 27-29**] *(England, on*** *Column 9, line 45-lines 51 and column 9, lines 65-column 10, lines 3; column 9, lines 27-29* ***discloses the following which meets the above limitation. First on column 9, lines 45-lines 51 the following has been disclosed.*** *The content provider 220 transmits a challenge message 4 to the DRMOS 205 asking for the identity of the CPU 201, the DRMOS 205, and the application 209 and this meets the limitation recited as "issuing a second challenge to the participant's computing device if the participant's computing device is determined to be trustworthy" because all subscribers shown on figure 2, ref. Num "200" provides some information to content providers shown on figure 2, ref. Num 220, before they receive any challenge from the content providers that will qualify them to be trustworthy"; Furthermore The DRMOS 205 transmits a response message 5 containing a certificate 202 for the CPU 201, its own*

identity 206, and the rights manager certificate 210 for the application 209.Furthermore on column 9, lines 65-column 10, lines 3, the following has been disclosed. "The certificate 202 is signed using the private key of the CPU 201. The content provider 220 examines the CPU certificate 202, the DRMOS identity 206, and the properties specified in the rights manager certificate 210 to determine whether it should establish a trust relationship with the DRMOS 205 on the subscriber computer 200." Note that as it is described on column 9, lines 27-29, certificate 210 identifies the trusted application.

Furthermore the primary reference on the record namely Trusted Computing discloses a method, in which the challenge is issued by a server *[figure 1, ref. Num "12"]* ***with which the participants computing device*** *[figure 1, ref. Num "14-16]* ***is in communication.*** *[figure 1, ref. Num "18" and See also page 5, under the title "Remote Attestation, up to page 6, first paragraph] ("TCPA remote attestation allows an application* ***(the "challenger")*** *to trust a remote platform. This trust is built by obtaining integrity metrics for the remote platform, securely storing these metrics and then ensuring that the reporting of the metrics is secure. For example, before making content available to a subscriber, it is likely that a service provider will need to know that the remote platform* ***is trustworthy.*** *The service provider's platform (the "challenger") queries " the remote platform, meets the limitation "****issuing a first challenge to a participant's computing device to determine whether the participant's computing device is trustworthy****," During*

system boot, the challenged platform creates a cryptographic hash of the system BIOS, using an algorithm to create a statistically unique identifier for the platform. The integrity metrics are then stored. When it receives the query from the challenger, the remote platform responds by digitally signing and then sending the integrity metrics. The digital signature prevents tampering and allows the challenger to verify the signature. If the signature is verified, the challenger can then determine whether the identity metrics are trustworthy meets the limitation of ***"determining whether or not the participant's computing device is trustworthy"*** *If so, the challenger, in this case the service provider, can then deliver the content. It is important to note that the TCPA process does not make judgments regarding the integrity metrics. It merely reports the metrics and lets the challenger* ***make the final decision regarding the trustworthiness*** *of the remote platform.)*

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

a. U.S. Patent No. 6, 990,660 B2, Moshir et al discloses an automated method for at least attempting to update software in a system having a first target computer in a non-update state connected across a network to an update server in a pre-update state.

15. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

06/05/2008
/Samson B Lemma/
Examiner, Art Unit 2132

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132